应用说明 # 28

HID ***iCLASS*** 13.56 MHz 读/写非接触式智能卡和读卡器

HID ***iCLASS*** 13.56 MHz 读卡器、读卡器/写卡器和非接触式智能卡与现有的门禁系统兼容，并且通过与不同应用系统提供商的整合，可以在更多领域应用，如生物识别、考勤系统、电子货币及自动售买、HVAC 自动控制和记帐 、IT 安全认证、警卫巡逻、停车管理和医疗或服务记录储存。

HID ***iCLASS*** 读卡器可以将 13.56MHz RF 能量转换成电能，与无源 ***iCLASS*** 非接触式智能卡进行通讯。ISO 15693 标准可以实现更长的读取范围，同时又符合 FCC 能量输出限制。 由于认证密钥更大，加密功能更强，***iCLASS*** 提供的安全性比同类的 13.56MHz 技术，如 MIFARE®[1] 要高。与 MIFARE 的 48 位密钥相对，***iCLASS*** 使用 64 位密钥，而且 ***iCLASS*** 使用多种不同的密钥，并且可以使用 DES 或 Triple DES 在卡上加密储存的数据，而 MIFARE 是随意存储其密钥和数据。

本文档将做概括介绍，可以让你熟悉应用系统提供商、咨询商、经销商和最终用户是如何使用 ***iCLASS*** 功能的。要实现一项新的应用，需要“软件开发套件”以及厂家培训和认证。

iCLASS 读卡器

iCLASS 读卡器备有三种颜色：黑色、灰色和白色。它们还备有以下三种不同的规格用于各种不同的用途，见下所述。除不同的 LED 和蜂鸣器操作模式之外，这些读卡器还有许多其它配置选项，可以在工厂进行预设置，或使用 HID 技术支持部门提供的专用配置卡在现场进行修改。

iCLASS 读卡器产品可以分为三类：只读型、读/写型和 OEM 型。

只读型（韦根输出）

R10 – 用在门框、竖框和其它受限制的空间上
R30 – 用在 80mm 正方形欧洲或亚洲背盒上
R40 – 用在美国 J-box 上，另外还配有欧洲/亚洲安装孔

这些读卡器都配有标准韦根接口，可以配合多数门禁系统使用。它们可以读取工厂在 ***iCLASS*** 卡、密钥和标牌上编码的 HID 韦根格式数据，也可以使用 Philips S50 或兼容的 IC，并将其转换为韦根数据来读取 MIFARE 卡中的 CSN（卡序列号）。

读/写型（韦根 + RS232）

RW300 – 用在 80mm 正方形欧洲或亚洲背盒上
RW400 – 用在美国 J-box 上，另外还配有欧洲/亚洲安装孔

除韦根接口外，这些读卡器还配有 RS-232 接口，可以用来连接主机系统（PC 或微控制器）。通过使用 ***iCLASS*** 串行协议，应用系统提供商可以读取、写入或修改 ***iCLASS*** 凭证卡应用区域内存储的信息。

OEM 型（韦根 + RS-232 或 TTL）

OEM100 – 集成到配有要求韦根或 TTL 的有限空间和应用系统的第三方设备中 [2]
OEM300 – 集成到配有要求韦根或 RS-232 的应用系统的第三方设备中

这些模块由共形镀膜电路板组成，可以集成到其它产品，如生物识别读卡器、考勤系统终端的外壳上。这两种型号均配有标准韦根接口。另外，OEM100 还配有双向 TTL 接口，OEM 300 配有 RS-232 接口。这两种型号都支持主机控制的读/写功能，以及开路集电极 (Open Collector) 逻辑输出的主机控制。这些电路板包含有集成天线和 LED（可以被去掉）。没有提供扬声器。

iCLASS 凭证卡

iCLASS 凭证卡可以使用“HID 企业 1000”或任何韦根格式的数据在工厂进行编程，以配合门禁系统使用。这些凭证卡备有 2 千位（256 字节）或 16 千位（2 千字节）的内存，16 千位的版本备有 2 或 16 个应用区域（请参阅“卡内存组织”中的部分）。

iCLASS 非接触式凭证卡可以分为三类：ID 卡、密钥和标牌。

iCLASS 200X – 204X – 卡 这些白色、光面、层压的 PVC 卡在尺寸和厚度上符合 CR80 和 ISO 7810 标准，可以使用染色升华或热传输卡打印机在两面打印，也可以由厂家进行自定打印。它们也可以进行插槽穿孔用于垂直方向。门禁控制 ID 号可以通过喷墨打印或激光刻印方式印制在卡上。这些卡是不可雕饰的。

iCLASS 卡可能只配备了 ***iCLASS*** 技术，或者采用了多项技术，允许从旧系统，包括磁条、接触式芯片、HID 感应卡和韦根卡的升级（或配合使用）（请参阅“订购指南）。采用韦根技术的 ***iCLASS*** 不能同时配合接触式芯片或感应卡使用，并且需要更厚的厚度（0.037” 或 0.94mm）。

iCLASS 205X – 密钥 这些精密铸造的聚碳酸酯密钥包括有一个插槽，可以配合多数钥匙圈或徽章夹。门禁控制 ID 号可以使用喷墨打印机印制在标牌上。

iCLASS 206X – 标牌 这些很薄的聚碳酸酯卡直径为 1.285” (32mm)，厚度为 0.070” (1.78mm)，并备有实用的背面粘贴。这些标牌不可拆除（若拆除标牌就会损坏它）。这些标牌可以粘贴到 PDA、手机、公文包和其它个人小物品的非金属表面。它们也可以粘贴到使用其它技术，如感应、韦根、钡铁氧体或磁条的现有 ID 或门禁控制卡的背面，而且无需高成本的徽章重制就可以升级到 ***iCLASS*** 技术。这些标牌并非与所有插入式、磁条或自动吸入式读卡器兼容，强烈建议你要求非功能性或功能性的样本标牌测试想要的应用。

MIFARE 卡

iCLASS 读卡器另外还提供了只从以下类型 MIFARE 卡读取卡序列号 (CSN) 的功能：

- HID 型号 1430 MIFARE
- HID 型号 1431 MIFARE，备有 HID 125 kHz 感应卡
- 使用 Philips S50 或兼容 Infineon Card IC 的卡
- 使用 Philips Mifare Pro IC 的卡
- 使用 Philips Mifare Lite 的卡

这项功能对于客户已经大量配置了 MIFARE 卡，并且还想将这些卡用于门禁系统的应用系统来说是非常有用的。当 MIFARE 读卡器，如 HID 6055B 也能够用于实现这一功能时，使用 ***iCLASS*** 读卡器的好处是：

- 成本低（***iCLASS*** 不需要 Philips 编码芯片）
- 读取范围提高（提高约 25%）

- 可以读取或升级到 ***iCLASS*** 技术

CSN 输出模式	说明：	备注
0	32 位，	将 32 位 CSN 输出为韦根数据（首先是 MSB）
1	32 位反向 (6055A)	以相反顺序将 32 位 CSN 输出为韦根数据（以匹配 HID MIFARE 读卡器型号 6055A）
2	26 位	输出由 16 个低位 32 位 CSN、固定 8 位地址号以及开始和结束奇偶位组成的 26 位韦根数据。地址号默认为 001，但可以使用配置卡进行修改。
3	34 位	将 32 位 CSN，以及开始和结束奇偶位输出为韦根数据。
4	40 位	将 32 位 CSN 以及 8 位校验和输出为韦根数据。

图 1 – MIFARE 卡序列号输出模式选项

iCLASS 读卡器可以按照不同的格式（图 1）将 MIFARE 卡 32 位卡序列号 (CSN) 输出为韦根数据，这些格式可以在工厂配置（请参阅“订购指南”），也可以在现场使用配置卡进行配置。

如果不是 CSN，则 ***iCLASS*** 读卡器将不能读取 MIFARE 卡存储的任何数据，并且不能写入到 MIFARE 卡。

iCLASS 卡随机的唯一 64 位 CSN 会专门用于防冲突和密钥变化。与 MIFARE CSN 不同的是，HID ***iCLASS*** CSN 绝对不会由读卡器作为韦根数据进行传输。这主要是因为多数门禁系统控制面板不能接受 64 位数字，以及 CSN 也不安全。

iCLASS 读卡器可以读取混合配置的 MIFARE 和 ***iCLASS*** 卡。***iCLASS*** 读卡器可以从 ***iCLASS*** 卡输出 HID 编码的数据，可以根据配置输出 MIFARE CSN。这将要求门禁系统控制面板能够接受多种格式的韦根数据。对于自定密钥的卡和读卡器则不能使用这项功能。

硬件接口

iCLASS 读卡器配备有 18" 屏蔽 22AWG 辫形线，具有如下面图 2 所示的电线颜色和功能。OEM 模块通过透孔为焊接垫提供了相同的连线。

红色	+DC (10-16 VDC)
黑色	接地
绿色	数据 0
白色	数据 1
导管	**屏蔽接地
橙色	*绿色 LED
棕色	*红色 LED
黄色	*扬声器
蓝色	*保持
紫色	***开路集电极 (Open Collector)
灰色	***RX（串行接收）
红色/绿色	***DSR（未使用）
粉红色	***TX（串行传输）
红色/黄色	***DTR（未使用）

* 可选连接 Connections. ** 导管线可以是使用单独电源时的数据返回线。 *** 在 R10、R30 和 R40 上未使用

图 2 – ***iCLASS*** 线路连接

防撬开关

当配合连接到外部报警系统的磁簧片开关使用时，内部磁体可以提供撬门指示（R10 除外）。在安装板左侧的背后找出该开关，它位于安装孔的中间（图 3）。建议的磁开关包括：Ademco 945T、Sentrol 1038T、GRI 100T、110T 或 Aleph DC-2531。这不适用于 OEM 模块。

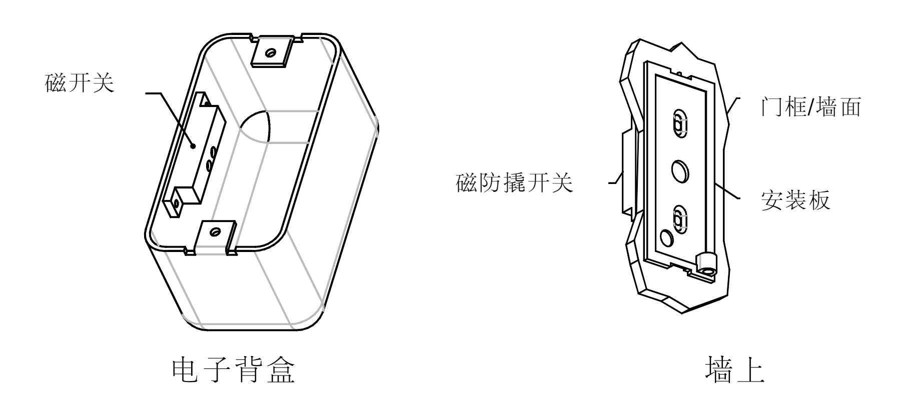


图 3 – 防撬开关安装

电源

iCLASS 读卡器需要 12 VDC 直线型电源，可以在 10-16VDC 范围内操作。就所有 RFID 读卡器而言，直流输入电源上的任何噪音都会影响性能和读取范围。建议不要切换电源或带整流器的变压器。

平均电量消耗 (75mA) 高于感应卡。由于“发光条”背后的 LED 阵列需要电能，因此电量消耗 (250-300 mA) 也比较高。

韦根、LED 和扬声器连接

韦根连接对于 HID 感应读卡器来说都是相同的。“时钟与数据”输出不会提供。LED 和扬声器操作可以配置用于内部或外部控制、单线或双线操作，而 LED 通常为绿色、红色或关闭。当压下（接地，或保持到逻辑低端，低于 2.5VDC）时，会启动 LED 和扬声器输入。读卡器可以使用想要的 LED/扬声器配置进行重新排序（请参阅“订购指南”）。

注意，当韦根电缆太长时，可能需要在电缆屏蔽的两端接地（或读卡器和面板接地），以便为读卡器及其电源（或面板）提供一个公共参考点。

扬声器可以产生音调和音调序列，也可以高，也可以低。这一项可以在工厂配置，也可以使用配置卡在现场配置。输入端是一个逻辑控制线，实际音调产生由读卡器的微处理器控制。没有外部音频输入。

保持输入

“保持输入”是一条控制线，当压下时 [3]，会关闭 RF 收发电路，直到线路被释放。这个输入端可以连接到车辆环路检测器的接触点或逻辑输出端，以便读卡器在车辆出现之前不会接受卡。另外，当线路压下时，读卡器会缓冲一个卡读取（忽略后来的读取），直至线路释放。这也可以使用配置卡选择。

开路集电极 (Open Collector) 输出

这个输出端通常是一个通过 RS-232 或 TTL 输入由串行命令控制的开路逻辑输出。（在 R10、R30 和 R40 型号没有。）这一电晶体开关提供了一个控制能由开关关闭来操作所有设备或逻辑输入的方法，对于在读卡器位置不提供延迟的非门禁控制应用系统是非常有用的。这个输出端可以是闭锁、解锁或暂时闭锁 1 – 255 秒。

开路集电极输出可以切换到最高 50mA，12VDC（最大 13.8VDC）。如果负载较大，则必须使用插入延迟。电涌振流器 (MOV) 应安装到这个输出端连接的所有电感负载上，以防瞬间脉冲损坏读卡器。

串行输入

RW300/400 配有串行 RS-232 接收和传输输入端可以连接到主机系统。没有提供信号交换线路。主机串行地线可以连接到读卡器的电源接地输入端。OEM100/TTL 的 PCB 上有两个插脚，提供了 TTL 接口。

操作模式

HID 13.56 MHz 非接触式 ***iCLASS*** 读卡器/写卡器（RW400、RW300、OEM100 和 OEM300）备有两个操作模式：**安全模式**和**主机模式**。***iCLASS*** 只读读卡器（R10、R30 和 R40）只在“安全模式”操作。

> **安全模式** – 这个模式用于门禁系统控制面板。该读卡器可以按照韦根格式输出工厂编程的“HID 企业 1000”或任一韦根格式的卡数据（或 Mifare 32 位卡序列号）（和/或通过串行端口有选择地按照十六进制格式在读卡器/写卡器上输出）。在这种模式下，当出示卡时，读卡器在其自己的控制系统下操作。它也可以响应其 LED、扬声器和保持控制线路的判断。
>
> 通过像标准感应或韦根读卡器那样连接韦根输出，传统的门禁控制 OEM、集成器和安装器可以实现“安全模式”操作。韦根数据可以在工厂或使用现场编程器编程到 ***iCLASS*** 卡。“门禁系统”经销商应从 HID 获得培训和支持，帮助客户选择适当的 ***iCLASS*** 卡和读卡器。
>
> **主机模式** – 这个模式通常用于非门禁应用系统。它允许开发商或集成器读写 ***iCLASS*** 卡。实际应用程序（售卖、借记、转帐等）会驻留在主机或微处理器中－不会驻留在读卡器中。读卡器在主机设备的专门控制系统中操作，响应在 RS-232 或 TTL 端口接收到外部命令。
>
> 主机会控制卡读取、LED、扬声器、开路集电极和所有读/写操作。软件或固件必须包括一个程序环路，使读卡器可以定期查找进入 RF 磁场的卡。LED、扬声器和保持功能的控制线路也可以继续在这个模式中工作。
>
> ***iCLASS*** 使用 ISO 7816-4 协议，这也是接触式智能读卡器通讯的标准。
>
> “主机模式”操作可以由应用系统提供商实现，这些提供商可以从 HID 获得“软件开发套件”、培训和支持。

ISO 标准

iCLASS 可以使用不同的 ISO 标准与非接触式智能卡通讯。这些标准定义用来在卡和读卡器之间通讯的 RF 协议，并指定频率、调制深度和数据速率。***iCLASS*** 读卡

器能够使用 ISO 14443A（在 MIFARE 卡上），或在 ***iCLASS*** 卡上使用 ISO 1443B2 和 ISO 15693。14443A 或 14443B2 的优点是数据速率较快，但读取范围会缩小。***iCLASS*** 读卡器通常使用 15693，这是因为对于多数应用系统来说，数据速率已经足够了，而较广的读取范围更为重要。（也请注意，2K 卡只能使用 ISO 15693 进行通讯）。

iCLASS 读卡器会自动使用 ISO 14443A 和 ISO 15693 选择和进行通讯，具体情况视出示的是 MIFARE，还是 ***iCLASS*** 卡而定。在与 ***iCLASS*** 卡通讯时，可以使用配置卡将 ***iCLASS*** 读卡器设置为只使用 ISO 14443B2。***iCLASS*** 读卡器/写卡器可以使用 ***iCLASS*** 协议设置为基于“每个命令”基础的 ISO 14443B2 。

注意，个别 ISO 标准中的通讯功能不包括由各家芯片制造商用来保护卡上存储数据的专有加密方法。每个厂家，如 Philips 或 Infineon 会提供自己的包括了专有算法的读卡器“芯片组”。如果读卡器没有要求的芯片组，则它将不能读取卡上存储的数据，只能读取卡序列号。

将 ***iCLASS*** 用于非门禁系统领域

要将 ***iCLASS*** 读卡器/写卡器用于非门禁系统领域，如生物识别、考勤系统、售卖等，应用系统提供商必须编写或修改他们的应用系统来使用 ***iCLASS*** 协议。一旦做到这点，则应用系统提供商将会拥有一个集成的系统，这个系统由 PC 或专用终端设备上连接的 ***iCLASS*** 读卡器，或专用终端设备上嵌入的 ***iCLASS*** OEM 模块组成。

应用系统提供商也可以开发软件或通过其它方法，将他们的应用数据编程到 ***iCLASS*** 卡中，如生物识别系统的登记台，电子售卖系统的现金接收机或信用卡，或考勤系统的软件程序等。多数应用系统提供商可以将他们的设备插接到 ***iCLASS*** 读卡器/写卡器的 RS-232 接口。

由于 ***iCLASS*** 使用 ISO 7816-4 协议，因此对于那些已经在他们的应用系统中集成了接触式智能卡的应用系统提供商来说，这种集成会相对简单一些。在最初推出 ***iCLASS*** 产品时，一些生物识别系统的厂家已经成功完成了与 ***iCLASS*** 的集成。

iCLASS 软件开发商套件提供有协议文档、编程指南和动态链接库 (DLL)、一些样本软件、销售演示程序，以及带电源和桌面支架的读卡器。注意，DLL 程序需要 PC 平台 – 低级协议命令可以用于微控制器和非 PC 平台。

每个联系 HID 的用户都可以获得 HID 推荐的其中一家能提供 turnkey 解决方案的应用系统提供商。

iCLASS 卡内存组织

在 ***iCLASS*** 卡上有三类内存区域（图 4）：

1 – 制造/配置区域
2 – 区域 1（HID 区域）
3 – 区域 2 – 16（应用系统提供商）

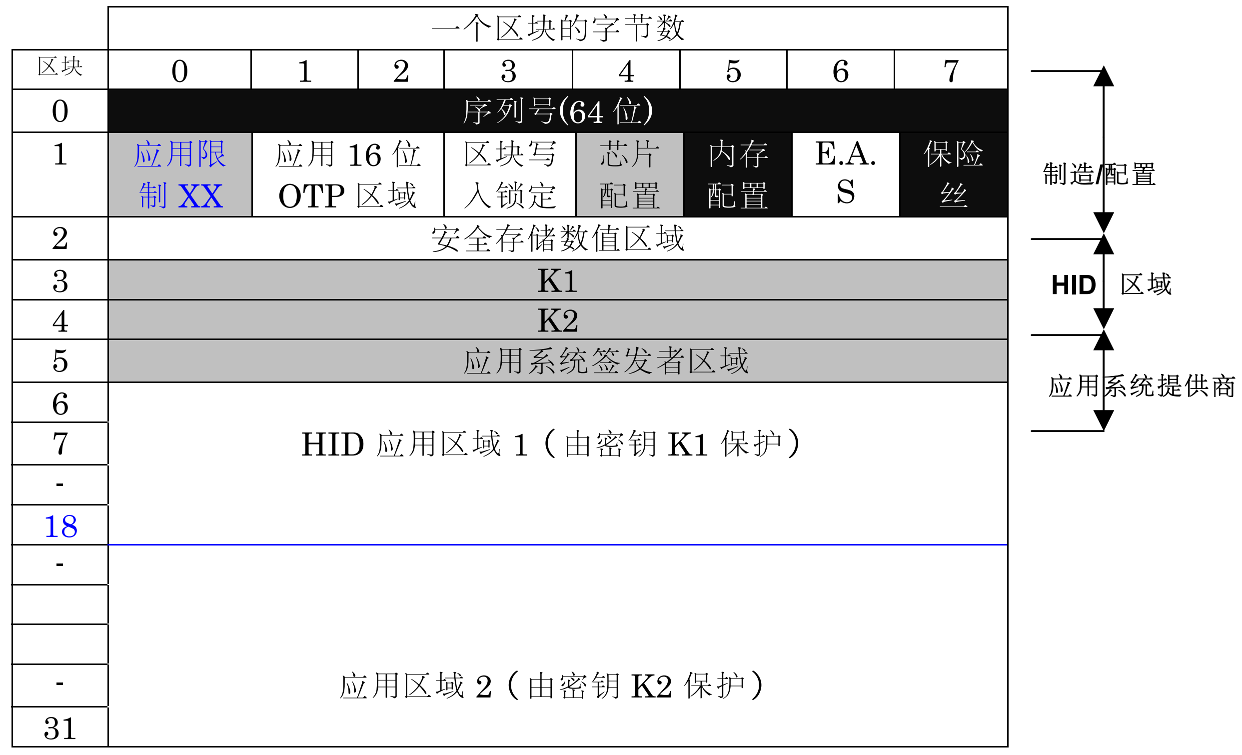
制造商/配置区域

每个卡的制造商/配置区域（图 4）为 6 个区块长（48 个字节），其中包括：

卡序列号（64 位唯一号码）
包括应用区域限制和保险丝的配置数据
安全存储数据区域
用于应用区域 1 和 2 的认证密钥
应用系统签发者区域（未使用）

应用区域

iCLASS 卡和标牌备有多种不同的配置。根据所订购卡的型号，***iCLASS*** 卡可能有 2 个或 16 个应用区域。在图 5 中“可用内存”是指还没有用于“制造/配置区域”或“应用区域 1 (HID)”的内存。



	一个区块的字节数							
区块	0	1	2	3	4	5	6	7
0	序列号(64 位)							
1	应用限制 XX	应用 16 位 OTP 区域		区块写入锁定	芯片配置	内存配置	E.A.S	保险丝
2	安全存储数值区域							
3	K1							
4	K2							
5	应用系统签发者区域							
6	HID 应用区域 1（由密钥 K1 保护）							
7								
-								
18								
-	应用区域 2（由密钥 K2 保护）							
-								
31								

图 4 – *iCLASS* 2K（或 16K/16 上的一对区域） 的内存映射

卡类型	应用区域	卡总内存量	可用区域	可用内存
2K/2	2	2 千位（256 字节）	1	104 字节
16K/2	2	16 千位 (2048 字节）	1	1896 字节
16K/16	16	16 千位(2048 字节）	15	1560 字节

图 5 – 不同卡类型的可用内存

应用区域 1

应用区域 1 有 13 个区块或 104 个字节（图 6），是专门为 HID 应用保留的，它包括有以下数据：

目录
门禁系统 ID（韦根格式数据）
PIN（将来）
密码（将来）
APB 状态（将来）
区域控制（将来）
用户字段 1 – 4（16 字节，每个）

区块		
6	HID 应用目录	HID 扩展应用目录
7	HID 门禁系统 ID	
8	HID 门禁系统 ID	
9	HID 门禁系统 ID	PIN
10	密码	
-	RFU	
18	RFU	

图 6 – HID 应用区域 1 的 *iCLASS* 内存组织

应用区域 2

这个区域用于用户应用，在长度上是固定的。

- 在 2K/2 卡上它是 13 个区块，104 个字节，可以包含存储的数值应用（图 4）。
- 在 16K/2 卡上它是 237 个区块或 1896 个字节，可以包含较大的储存数值应用，如生物识别模板、医疗记录或服务记录（图 7）。多项应用可以储存在一个区域内，但每个应用系统提供商必须注意不能覆盖其它数据，并且所有提供商必须共享认证密钥。

	一个区块内的字节数							
区块	0	1	2	3	4	5	6	7
0	序列号（64 位）							
1	应用限制 XX	应用 16 位 OTP 区域		区块写入锁定	芯片配置	内存配置	E.A.S	保险丝
2	安全存储数据区域							
3	K1							
4	K2							
5	应用系统签发者区域							
6	应用 1（由密钥 K1 保护）							
7								
-								
XX								
-	应用 2（由密钥 K2 保护）							
-								
255								

图 7 – ***iCLASS*** 16K/2 的内存映射

多应用卡

16K/16 卡有 16 个应用区域（图 8）。它们排列在 8 个页面，每个页面由一个制造区域和两个应用区域组成，制作格式与 2K/2 卡相似（图 4）。6 区块制造区域在所有 8 个页面上都存在，但从页面 0 开始的卡序列号用于所有密钥变化。每个页面上的制造区域存储其各自应用区域的相应密钥。

在页面 0，区域 1 为 HID 应用保留，区域 2 是固定的，就像在 2K/2 和 16K/2 卡上一样。在页面 1 – 7，区域 3 -16 供用户使用，而且在编程过程中每对应用区域（3 与 4、 5 与 6 等）之间的边界可以设置一次。

应用系统提供商可以在单个区域写入每项应用的数据，也可以在多个区域分布较大记录（如生物识别模板），在这种情况下，每个区域必须单独进行认证才能提取整个记录。使用多个区域时，建议在每对应用区域的 31 (1F Hex) 位置设置应用边界，以便第一个区域最大化（208 个字节），其它为零（图 4）。这样可以减少读取多个区域中存储数据需要的认证次数。

对于多数生物识别模板来说，在模板存储之后，16K/16 卡仍然有可用的应用区域。下面图 8 显示了生物识别模板可能在 16K/2 和 16K/16 卡上存储的方式。

16K/2 卡	
区域	内容
1	HID 应用
2	生物识别应用
	（未使用）

16K/16 卡		
页面	区域	内容
0	1	HID 应用
	2	生物识别应用
1	3	
	4	
2	5	
	6	
3	7	
	8	
4	9	售卖
	10	停车
5	11	借记
	12	图书馆
6	13	逻辑访问
	14	HVAC
7	15	个人信息
	16	个人信息

图 8 – 在 16K/2 和 16K/16 上存储应用数据

安全存储数值区域（存贷/借记应用）（区块 2）

虽然这项功能不能在 2K 或 16K/2 卡上使用，但可以在 6K/16 卡的页面 1-7 上使用。“安全存储数值区域”可以实现在 ***iCLASS*** 卡定义“钱包”以便用于售卖、转帐或其它电子货币用途。注意，当在某个页面上使用这项功能时，第一个密钥会用作借记密钥，每个会用作存贷密钥。由于这些密钥也可以用于保护该页面的第一和第二应用区域，因此建议你不要将这些区域用于不相关的应用。但是，这些区域可以用于存储相关数据，如帐号、货币、单位、贷款最高限额、帐户平衡和允许的最大购买数。

工厂默认编程

最初，所有卡都由 HID 制造部进行预编程。以后会提供现场编程器。工厂默认编程介绍如下：

- *序列号*：区块 0 是芯片的 8 字节唯一 ID。序列号不能由用户修改（ISO 标准）。
- *应用限制*：这个字节将被设置为数值 18 (12 Hex)，设置应用限制低于区块 18。HID 应用将一直驻留在应用区域 1 中。应用区域 1（HID 应用）由 13 个区块组成。对于 16K/16 卡，HID 应用将一直驻留在第一对应用区域的应用区域 1 中。16K/16 的区域 3-16 应用限制可以由应用系统提供商修改一次。

- *应用 16 位 OTP（一次性编程）区域：*未使用
- *区块写入锁定*：未使用 – 默认值 0xFF
- *芯片配置*：用于区别 2K 和 16K 卡。
- *内存配置*：用于区别 16K/16 和 16K/2 卡。
- *E.A.S*：未使用
- *保险丝*：如果这些是“熔化的”，则认证密钥不能在现场进行更改。
- *安全存储数据区域*：未使用（在 16K/16 卡的页面 1-7 上提供）
- *K1*、*K2*：在 HID 标准主密钥中 K1 和 K2 会变化。如果是 16K/16 卡，则剩余的 14 密钥也会被编程为默认值，也会与 HID 标准不同。每个密钥都将是不同的。通过将相应的默认密钥透露给它们，HID 将允许第三方厂商使用不同的应用区域。

  如果是 2K 卡，则一旦这些密钥在工厂编程，则它们以后将不能更修改。在 16K/2 和 16K/16 卡内，只要保险丝没有熔断，这些密钥就可以在现场修改。
- *应用 1*：为 HID 应用保留
- *应用 2*：（和多应用卡上的 3-16）为应用系统提供商保留
- *HID 应用目录*：定义 HID 门禁系统 ID 的长度和格式、PIN 的大小。指示 PIN 和 ID 是否已加密，如果已加密，则使用的是什么密钥和加密方案（DES 或 triple-DES）。
- *HID 扩展应用目录*：用来定义密码的格式以及剩余的应用区域。
- *HID 门禁系统 ID*：ID 用于 HID 门禁控制应用系统（通过韦根或 RS-232 输出）。最大长度为 144 位。
- *PIN*：48 位 PIN 为门禁控制应用系统保留（将来）
- *密码*：64 位数字，可以由程序员编写和读取（将来）
- *RFU*：为将来使用保留的内存区域。

iCLASS 安全

相互认证

相互认证是基于密码加密通讯的通用惯例。简单说来，卡和读卡器都需要对方有匹配的密钥，以便让读卡器“知道”持卡人是合法的，让卡“知道”读卡器已被授权读取其信息。

如果卡和读卡器只是简单地传输密钥给对方进行比较，则任一个具有技术背景的人以及调谐到读卡器频率的接收机都可以捕捉该信息，使他自己的智能卡可以获得出入许可。

正是由于这一原因，卡和读卡器都包含了复杂的密码算法，可以打乱传输的数据，使它无法理解。（算法是一种用来加密数字的数学公式。）为防止“黑客”对算法进行反向工程，卡和读卡器还备有随机数字生成器，并且每一个都会乘以一个随机

数字因数加入到算法中，因此如果你多次读取同一个卡，则传输的数据在每次都是不同的。每个卡包含有一个唯一的序列号，这个序列号用于加密卡上存储的密钥，从而使这个密钥在每个卡上都是唯一的。

当被读卡器选定时，卡会从随意发送其卡序列号（CSN）开始。如果发生多个卡出示的情况，则读卡器会使用这些 ID 号屏蔽其它卡，并选择一个要传输的卡。这个过程称作防冲突。（这也就解释了为什么 ***iCLASS*** 从不将序列号用于门禁系统 – 因为序列号是没有加密的。）

这时，假设读卡器和卡都是合法的，则现在它们有了一些公用的信息。两者都“知道”卡序列号，两者都有加密算法，并且两者都有密钥（读卡器有实际密钥，卡的密钥会在 CSN 中变化）。

读卡器使用 CSN、密钥、随机数字和算法计算 64 位数字。但是，它只发送前 32 位，称为“挑战”。卡接收 32 位“挑战”数字，然后使用这个数字、算法、CSN 和密钥重新创建 64 数字的后 32 位，并将其发送回到读卡器。读卡器会将卡内的响应与它在内存中存储的响应进行比较，如果它们相符，它会认证该卡。之后卡会通过发送“挑战”数字到读卡器来颠倒这个过程，会将响应发送回到卡。

一旦发生相互认证，则卡和读卡器会开始传输数据，并且读卡器会阅读或写入到已认证卡的扇区。

数据加密

在卡上 HID 应用区域存储的数据可以使用 DES 或三倍 DES 进行加密，这样即使万一密钥被“破解”，数据仍将会无法读取。

认证密钥

iCLASS 卡上存储的所有数据都由认证密钥进行保护。密钥基本上是一个密码，用来防止数据在未经授权的情况下读取或修改。***iCLASS*** 卡和读卡器使用 64 位密钥。一个密钥用来保护卡的每个应用区域。

HID 将韦根格式的卡数据编码到 ***iCLASS*** 卡的应用区域 1，并使用一个唯一的、变化的 HID 专有密钥（不会公布）保护这个数据。兼容密钥也会安全地存储在每个 HID ***iCLASS*** 读卡器上。

由于每个应用区域都有自己的密钥，因此 ***iCLASS*** 卡可以用来存储多个应用系统提供商的信息，并且会防止每个应用系统提供商意外修改另一个提供商的数据。建议应用系统提供商更改用于他们区域的默认密钥，他们负责其自己的密钥管理和数据加密。

iCLASS 应用系统提供商必须使用变化的密钥保护将要使用的应用区域。*iCLASS* 读卡器/写卡器通过执行密钥变化功能很容易做到这点。

iCLASS 读卡器可以存储最多 10 个认证密钥。即使在某一站点使用了 10 个以上的密钥，读卡器将只需存储用于其某一用途的那些密钥。新的密钥可以在需要时随时加载。

密钥管理

密钥管理的基本原则是：

- 每个卡，每个客户的密钥必须是唯一的
- 密钥必须安全地存储和加密
- 密钥绝对不能通过 RF 或 RS-232 随意传输
- 密钥绝对不能在没有保护的硬盘驱动器或内存芯片上读取

在使用“标准密钥管理”时，用来保护所有卡上应用区域 1 的密钥会使用加密算法、唯 一卡序列号和区域号码在 HID 标准主密钥中变化，以便每个卡上和每个应用区域内的密钥都是唯一的。相同的标准主密钥会安全地存储在读卡器上，并且绝对不会传输。由于一个主密钥用来创建所有卡和读卡器的密钥，因此包含标准密钥的 ***iCLASS*** 读卡器是可以互换的，并且相互兼容。由于在 ***iCLASS*** 读卡器中使用了加密和相互认证，因此这个密钥是极其安全的。

HID 自定密钥将附加的安全层添加到了基本 ***iCLASS*** 密钥变化和加密方案。某一站点的自定密钥会由 HID 分配给每个客户，取代标准密钥。对于 HID 应用区域，HID 的密钥管理系统使用专有算法从自定主密钥中生成 256 密钥数据库。CSN 会用来从密钥数据库的 8 个不同位置抽取字节来创建 64 位密钥。

在自定密钥站点的所有卡上，HID 会使用从自定密钥中变化得来的密钥对应用区域 1 进行保护，然后对所有要匹配的读卡器加上密钥。自定密钥和密钥数据库驻留在每个读卡器中。HID 在加密的数据库中保持自定密钥，这个数据库出厂时被存储在安全的位置，并且有一个备份存储在安全的离站位置。由于站点特定的主密钥用来对所有卡和读卡器加密钥，因此自定密钥的卡和读卡器是不能与另一个站点的卡或读卡器进行互换的，并且附加的卡和读卡器必须使用相同的密钥 ID 号排列顺序。

HID 将来会提供 ***iCLASS*** 卡编程器，这是一个连接到 PC，并运行 Windows 软件的特殊版本的读卡器（与 HID ProxProgrammer 相似）。这个编程器将允许最终用户或系统集成商在现场创建和保护自己的自定密钥，也会允许个性化数据编码和加密到每个卡 HID 应用区域的指定数据字段。注意，需要 16K/2 或 16K/16 卡。最终用户或系统集成商在购买自己的编程器时对系统安全负有完全责任。

有关密钥管理的更多信息，请参阅 HID 网站上的“***iCLASS*** 安全实现计划”（***iCLASS*** Security Implementation Plan）文档，网址：
www.hidcorp.com/iclass/index.html。